IPSec

A Basic Overview

IPSec Terms an Definitions

- Manual Keying
- IKE
- Phase I
- Phase II
- Quick Mode
- AH
- ESP
- ISAKMP

Manual Keying

Manual Keying, auch als preshared key bezeichnet, bedingt den Austausch der Schlüssel auf beiden Endpunkten vor der Herstellung des Tunnels. Die Schlüsselinformationen können möglicherweise relativ leicht erraten werden und die Sicherheit ist dadurch erheblich beeinträchtigt.

IKEs

- IKE dient der automatischen Schlüsselverwaltung
- IKE verwendet Prot 500/udp oder 4500/udp bei NAT-Traversal
- IKE arbeitet in 2 Phasen:
  - Aushandeln einer Security Association (SA) Aggressive Mode oder Main Mode
  - Erzeugen einer SA für IPSec mit Quick Mode

IKE Phase I – Main Mode

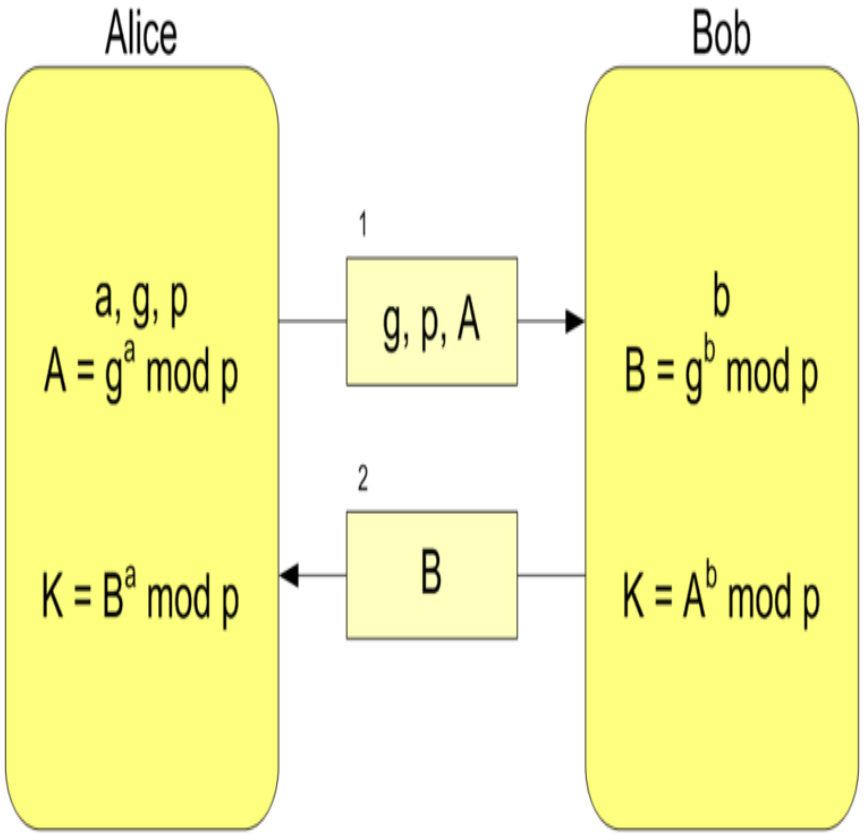
- Der Initiator sendet Vorschläge für mögliche Authentifizierungs- und Verschlüsselungsverfahren
- Der Responder wählt die sichersten Verfahren aus
- Der Initiator sendet den Public Part des Diffie-Hellmann-Keys und eine Nonce (Zufallswert)
- Der Responder sendet seinen Public Part des Diffie-Hellmann-Keys und eine Nonce
- Authentifizierung mittel einem Hashwert
  - Hashing der Nonce
  - Hashing der IP Adresse
  - Hashing der verwendeten Verschlüsselungsverfahren
  - Hashing der versandten Nachrichten

IKE Phase I – Aggressive Mode

- Der Initiator sendet Vorschläge für mögliche Authentifizierungs- und Verschlüsselungsverfahren
- Der Responder wählt die sichersten Verfahren aus
- Der Initiator sendet den Public Part des Diffie-Hellmann-Keys
- Der Responder sendet seinen Public Part des Diffie-Hellmann-Keys
- Übertragung der Hashwerte der PSKs im Klartext

Diffie-Hellmann

- **Alice und Bob einigen sich auf *p* = 13 und *g* = 2.**
- **Alice wählt die Zufallszahl *a* = 5. Bob wählt die Zufallszahl *b* = 7.**
- **Alice berechnet *A* = 25mod 13 = 6 und sendet dieses Ergebnis an Bob.**
- **Bob berechnet *B* = 27mod 13 = 11 und sendet dieses Ergebnis an Alice.**
- **Alice berechnet *K* = 11^5mod 13 = 7.**
- **Bob berechnet *K* = 6^7mod 13 = 7.**
- **Beide erhalten das gleiche Ergebnis *K* = 7.**



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Security Association

- Eine Vereinbarung der beiden Teilnehmer über:
  - Deren Identifikation
  - Verschlüsselungsalgorithmen für IPSec
  - Von welchen Netzwerk erfolgt die Verbindung
  - Zu welchem Netzwerk geht die Verbindung
  - Wann werden die Schlüssel erneuert
  - Wann wir erneut Authentifiziert

IKE Phase II – Quick Mode

- Nach abgeschlossener Phase I sind bereits alle Informationen ausgetauscht, um erfolgreich zu verschlüsseln
- Der Initiator sendet einen Vorschlag (Proposal) über die zu verwendenden Verschlüsselungs- und Hashverfahren
- Der Initiator überträgt die Proposal mit einem Hash und seiner Nonce
- Ein erneuter Diffie-Hellmann-Schlüsselaustausch findet statt
- Die alten Secrets werden gelöscht
- Eine neue SA ist generiert
- Durch eine komplette Neuverhandlung aller Informationen kann niemals von einer vorigen Vereinbarung auf die neue Vereinbarung geschlossen werden = Perfect Forward Secrecy

Transport Mode vs. Tunnel Mode

- Im Transport Mode wird der Verkehr zwischen zwei Hosts verschlüsselt
- Es wird nur der IP Payload dieser Hosts verschlüsselt
- Im Tunnel Mode wird das gesamte IP Packet verschlüsselt
- Die Tunnelendpunkte transportieren auch den Verkehr anderer Maschinen

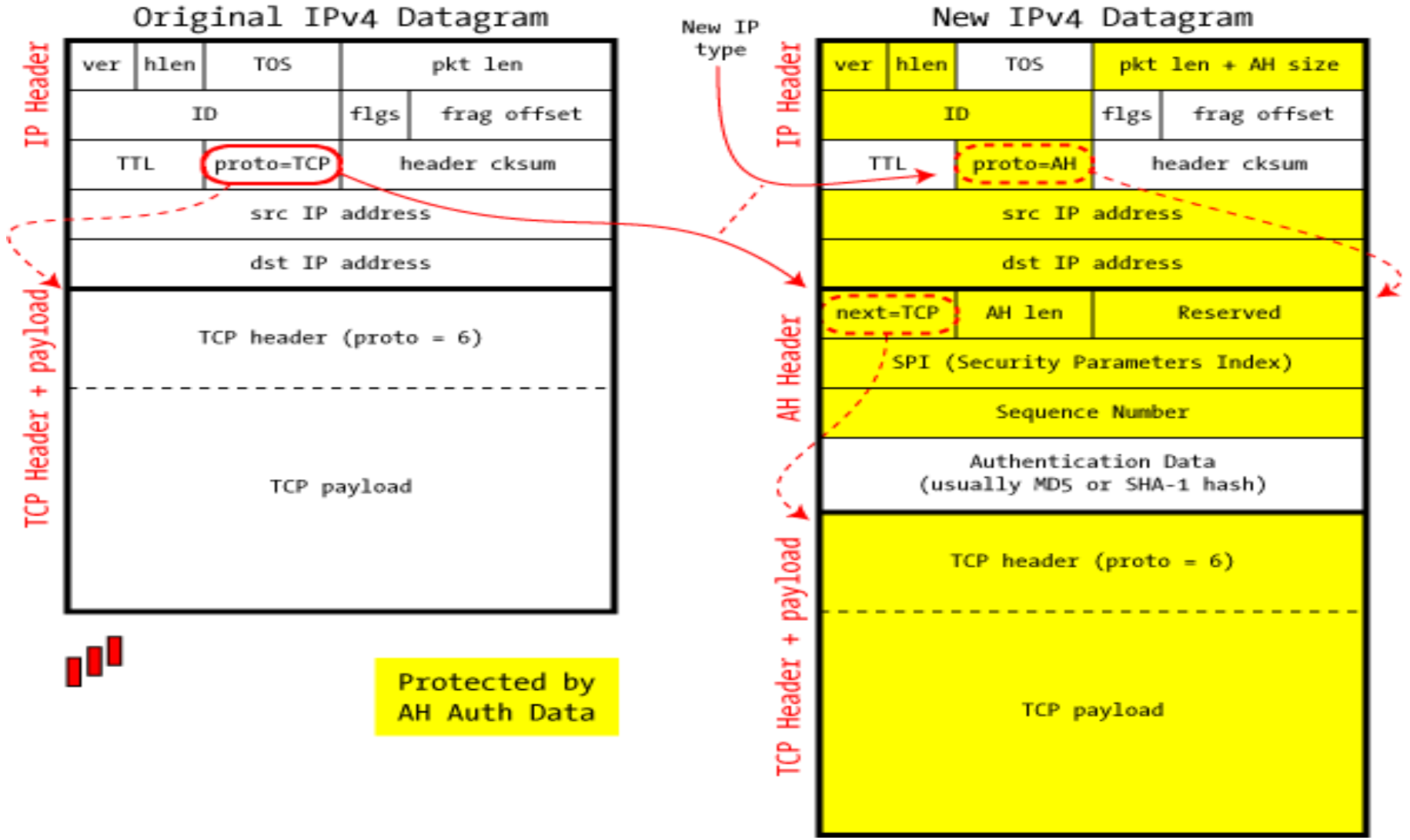
Transport Mode vs. Tunnel Mode

- Im Transport Mode wird der Verkehr zwischen zwei Hosts verschlüsselt
- Es wird nur der IP Payload dieser Hosts verschlüsselt
- Im Tunnel Mode wird das gesamte IP Packet verschlüsselt
- Die Tunnelendpunkte transportieren auch den Verkehr anderer Maschinen

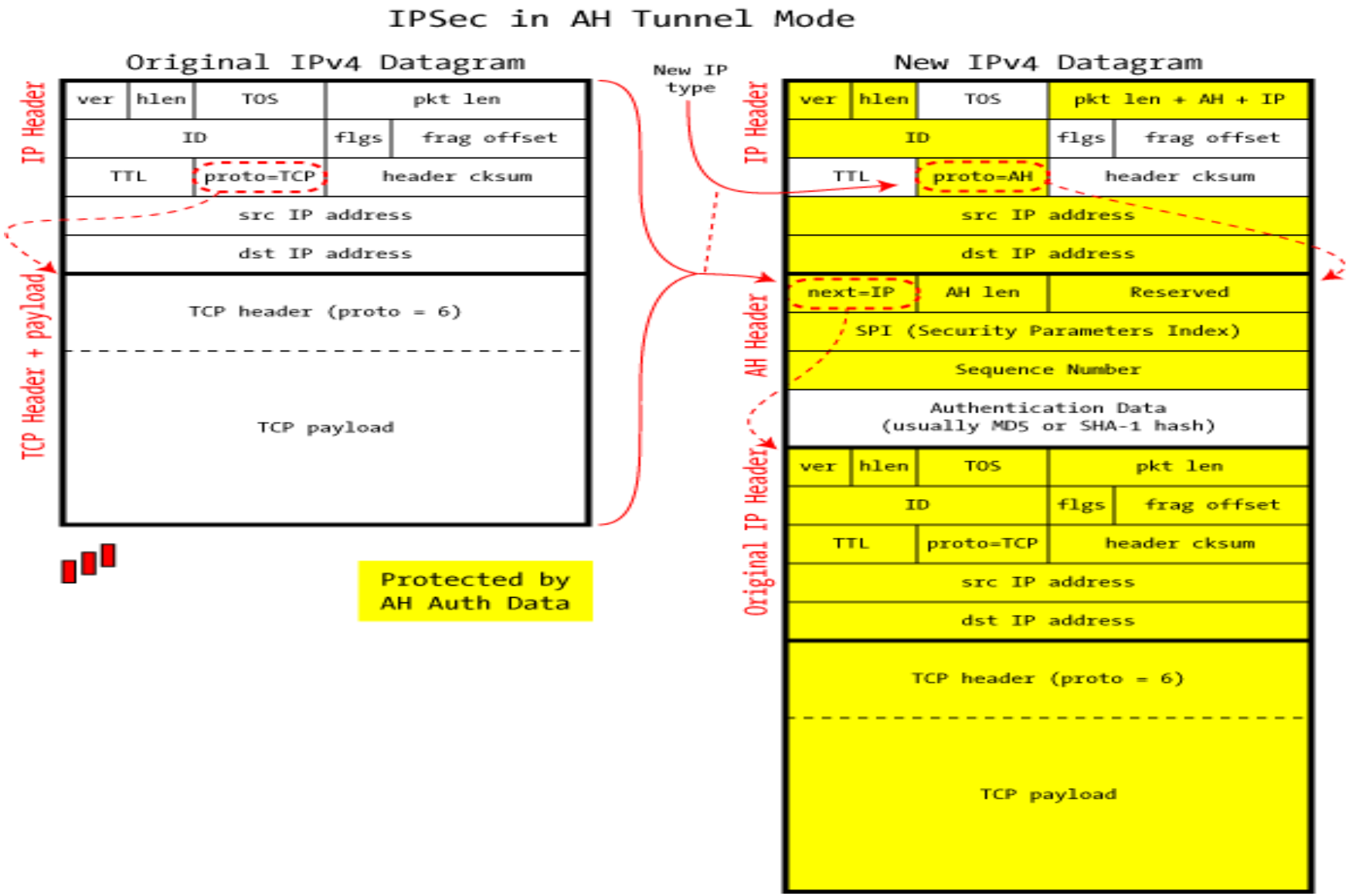
AH: Authentication Header

- AH authentifiziert Pakete und prüft diese auf Veränderungen während des Transports
- Ein Hashwert wird über nahezu alle Felder des IP Pakets gelegt (mit Ausnahme von TTL und Checksum)
- Der Hash wird in einem neuen IP Feld des AH Header gespeichert und an die Gegenstelle übertragen
- Der AH Header wird zwischen dem ursprünglichen IP Header und dem Payload eingefügt

AH: Transport Mode

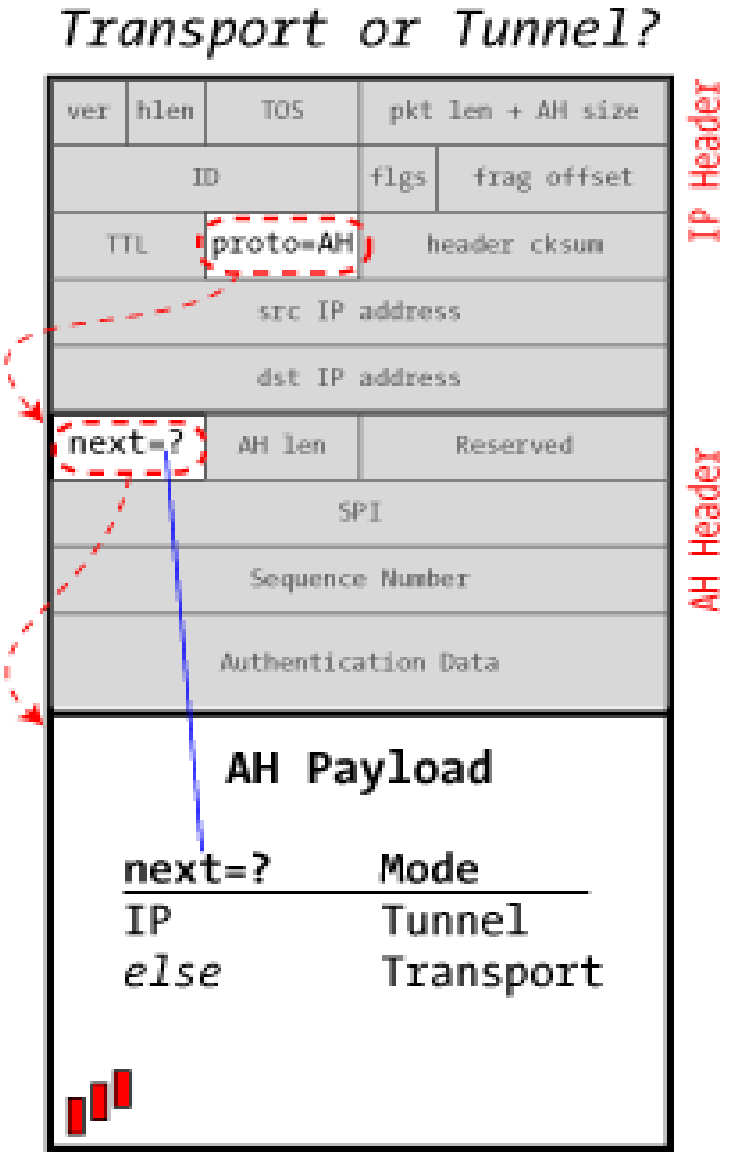


AH: Tunnel Mode

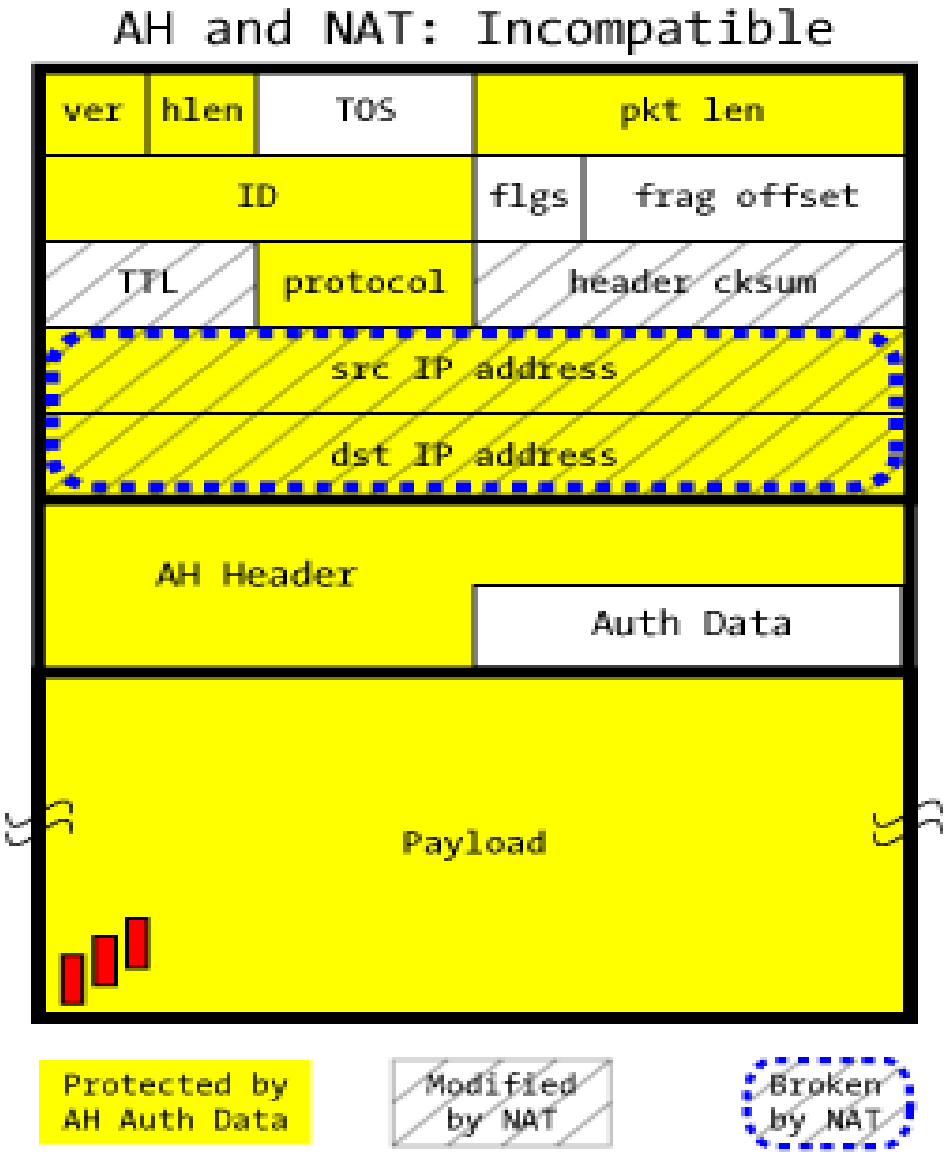


AH: Transport oder Tunnel?

- Es gibt keinen expliziten Transport bzw. Tunnel Flag
- Ist der next-header Wert IP, dann wird der komplette IP Header signiert, dies entspricht dem Tunnel Mode
- Jeder andere Wert im next-header entspricht dem Transport Mode

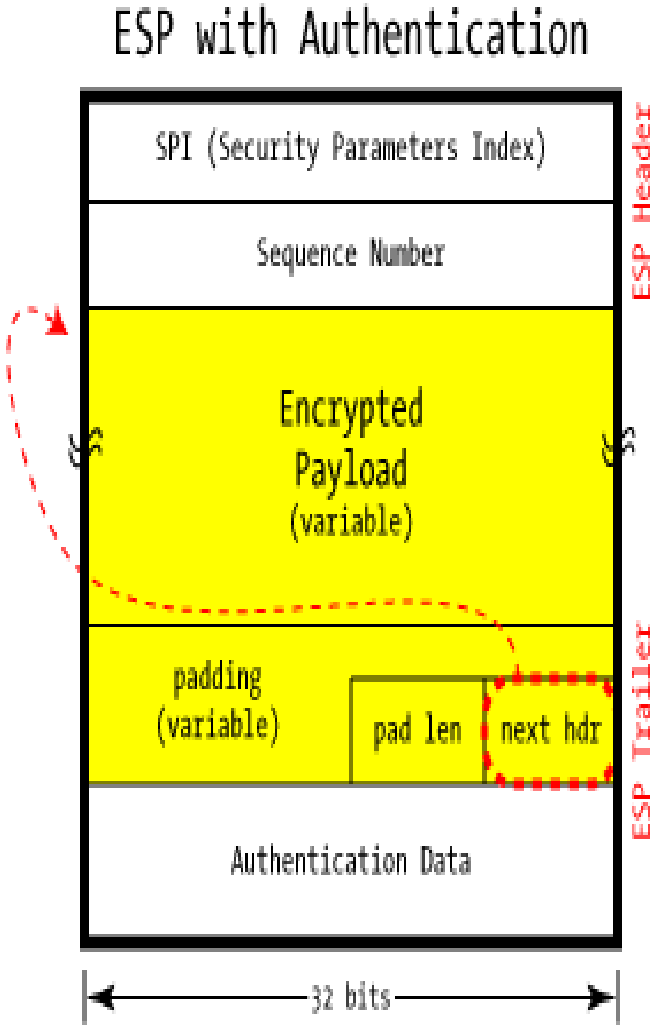


AH: Nicht NAT-Kompatibel



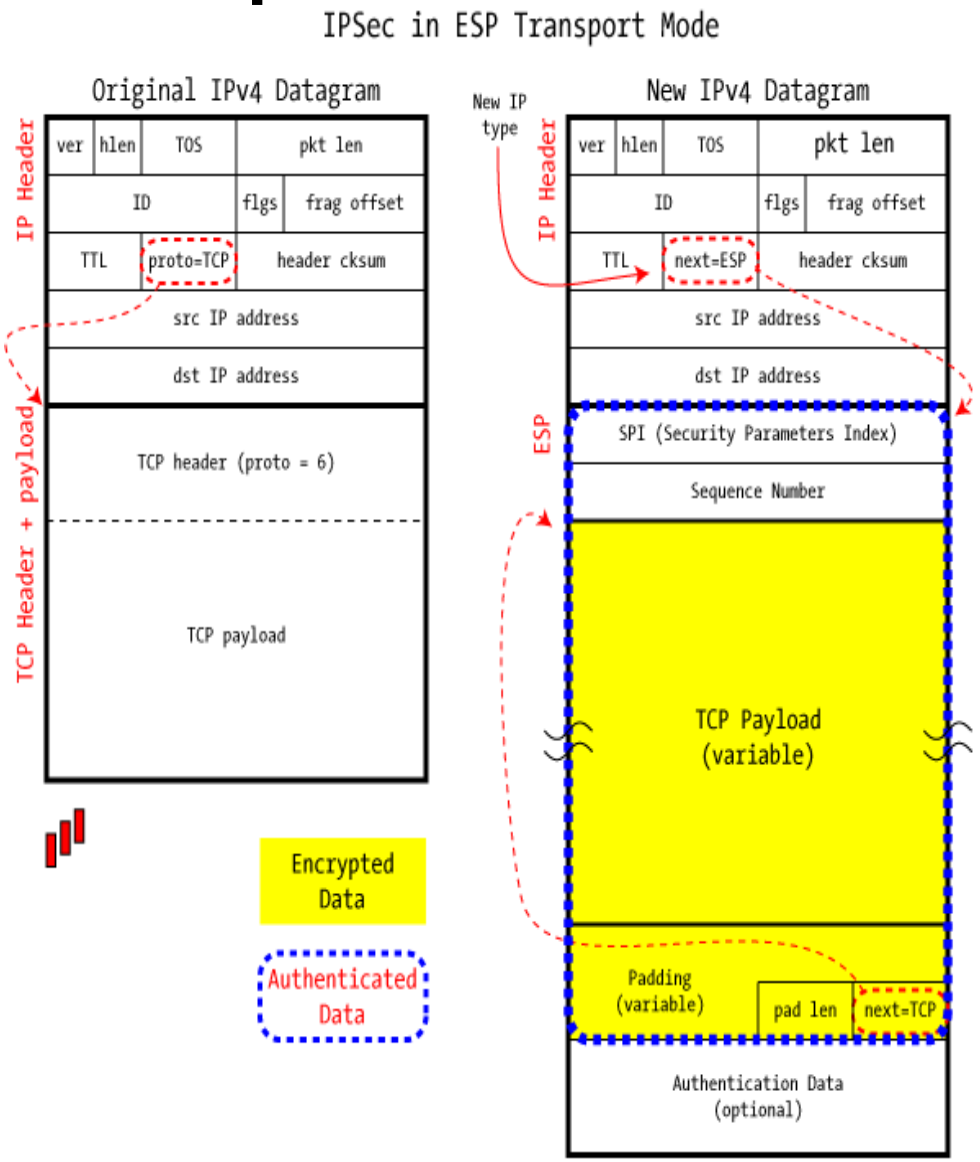
ESP: Encrypted Security Payload

- ESP umgibt den gesamten Payload, es wird nicht einfach eingefügt
- ESP kann Verschlüsselung und Integrität sicherstellen. Die Integrität betrifft allerdings nur den verschlüsselten Payload und dessen Header – nicht das gesamte IP Paket
- Wenn ein Angreifer ein ESP Paket untersucht kann er nicht erkennen was im Paket enthalten ist. Ob Authentifizierung erforderlich ist, ist für ihn nicht zu erkennen
- Manchmal können Flags ausserhalb des Payloads hinweise auf transportierte Daten liefern, z.B. QoS Tags bei VoIP



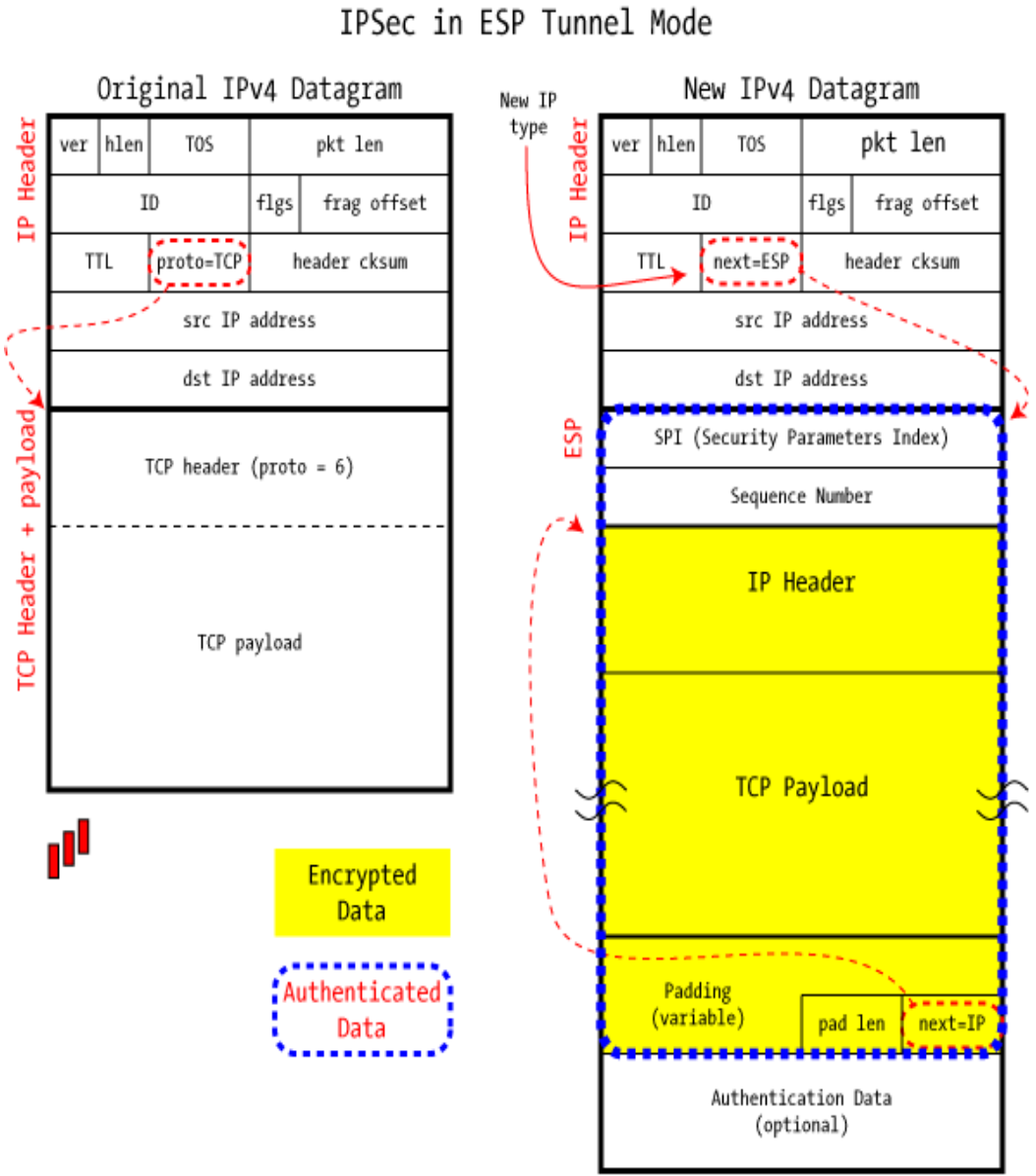
AH: ESP Transport Mode

- Es wird nur der Payload verschlüsselt
- IP Adressen bleiben unberührt
- Dient der Host zu Host Kommunikation



AH: ESP Tunnel Mode

- Ein gesamtes IP Paket wird innerhalb von ESP verschlüsselt
- Da das next-header Field als Teil des IP Pakets verschlüsselt ist kann Tunnel und Transport Mode von außen nicht erkannt werden



ISAKMP

- ISAKMP oder auch DPD (Dead Peer Detection) soll unbeabsichtigte Verbindungsabbrüche entdecken
- Innerhalb von IKE Port 500/udp werden Notify-Messages ausgetauscht, um das Vorhandensein der Gegenstelle zu entdecken
- Wird ISAKMP nicht verwendet und eine Verbindung bricht ab wird von der Gegenstelle ein erneuter Verbindungsaufbau verweigert, weil noch eine gültige SA vorhanden ist.
- DPD gewährleistet eine dauerhaften Verbindungscheck und wird auch als ISAKMP-Keepalive bezeichnet